IN THE CLAIMS:

1. (Original) A method of verifying the integrity of unauthenticated code, comprising:

receiving automatically authenticated code, the automatically authenticated code including an embedded first hash value of the unauthenticated code;

receiving the unauthenticated code;

generating a second hash value of the unauthenticated code;

comparing the first hash value and the second hash value; and

verifying the integrity of the unauthenticated code if the first hash value and the second hash value match.

2. (Previously Presented) The method of claim 1, wherein the automatically authenticated code is compiled platform independent code and wherein the unauthenticated code is native code.

3. (Previously Presented) The method of claim 1, wherein the automatically authenticated code is a platform independent application or applet and wherein the unauthenticated code is a dynamically linked library.

4. (Original) The method of claim 1, wherein the first hash value is obtained using a hashing function and wherein generating a second hash value of the unauthenticated code includes using the same hashing function as was used to obtain the first hash value.

5. (Original) The method of claim 4, wherein the hashing function is identified based on information stored in the automatically authenticated code.

6. (Original) The method of claim 1, further comprising:

executing the automatically authenticated code using a virtual machine; and

sending a request to a server from which the automatically authenticated code was received, the request being for the unauthenticated code.

7. (Original) The method of claim 1, wherein, if the first hash value and the second hash value do not match, the method further comprises:

receiving the unauthenticated code again;

generating a third hash value of the unauthenticated code; and

comparing the first hash value and the third hash value.

8. (Original) The method of claim 7, wherein if the third hash value and the first hash value do not match, the method further comprises:

comparing the second hash value and the third hash value; and

if the second hash value and the third hash value match, determining that the unauthenticated code has been corrupted intentionally.

9. (Original) The method of claim 8, wherein if the second hash value and the third hash value do not match, it is determined that the unauthenticated code has been corrupted unintentionally.

10. (Original) The method of claim 1, wherein the method is implemented in a virtual machine associated with a web browser on a client device.

11. (Original) An apparatus for verifying the integrity of unauthenticated code, comprising:

a virtual machine; and

an unauthenticated code verification element, wherein the virtual machine receives automatically authenticated code, the automatically authenticated code including an embedded first hash value of the unauthenticated code, and receives the unauthenticated code, and wherein

the unauthenticated code verification element generates a second hash value of the unauthenticated code, compares the first hash value and the second hash value, and verifies the integrity of the unauthenticated code if the first hash value and the second hash value match.

12. (Previously Presented) The apparatus of claim 11, wherein the automatically authenticated code is compiled platform independent code and wherein the unauthenticated code is native code.

13. (Previously Presented) The apparatus of claim 11, wherein the automatically authenticated code is a platform independent application or applet and wherein the unauthenticated code is a dynamically linked library.

14. (Original) The apparatus of claim 11, wherein the first hash value is obtained using a hashing function and wherein the unauthenticated code verification element generates a second hash value of the unauthenticated code using the same hashing function as was used to obtain the first hash value.

15. (Original) The apparatus of claim 14, wherein the hashing function is identified by the unauthenticated code verification element based on information stored in the automatically authenticated code.

16. (Original) The apparatus of claim 11, wherein the virtual machine executes the automatically authenticated code and
sends a request to a server from which the automatically authenticated code was received, the request being for the unauthenticated code.

17. (Original) The apparatus of claim 11, wherein, if the first hash value and the second hash value do not match, the virtual machine receives the unauthenticated code again, the unauthenticated code verification element generates a third hash value of the unauthenticated code and compares the first hash value and the third hash value.

18. (Original) The apparatus of claim 17, wherein if the third hash value and the first hash value do not match, the unauthenticated code verification element compares the second hash value and the third hash value and, if the second hash value and the third hash value match, determines that the unauthenticated code has been corrupted intentionally.

19. (Original) The apparatus of claim 18, wherein if the second hash value and the third hash value do not match, the unauthenticated code verification element determines that the unauthenticated code has been corrupted unintentionally.

20. (Original) The apparatus of claim 11, wherein the virtual machine and the unauthenticated code verification element are associated with a web browser on a client device.

21. (Original) A computer program product in a computer readable medium for verifying the integrity of unauthenticated code, comprising:

first instructions for receiving automatically authenticated code, the automatically authenticated code including an embedded first hash value of the unauthenticated code;

second instructions for receiving the unauthenticated code;

third instructions for generating a second hash value of the unauthenticated code;

fourth instructions for comparing the first hash value and the second hash value; and

fifth instructions for verifying the integrity of the unauthenticated code if the first hash value and the second hash value match.

22. (Previously Presented) The computer program product of claim 21, wherein the automatically authenticated code is compiled platform independent code and wherein the unauthenticated code is native code.

23. (Previously Presented) The computer program product of claim 21, wherein the automatically authenticated code is a platform independent application or applet and wherein the unauthenticated code is a dynamically linked library.

24. (Original) The computer program product of claim 21, wherein the first hash value is obtained using a hashing function and wherein the third instructions for generating a second hash value of the unauthenticated code include instructions for using the same hashing function as was used to obtain the first hash value.

25. (Original) The computer program product of claim 24, further comprising instructions for identifying the hashing function based on information stored in the automatically authenticated code.

26. (Original) The computer program product of claim 21, further comprising:

sixth instructions for executing the automatically authenticated code using a virtual machine; and

seventh instructions for sending a request to a server from which the automatically authenticated code was received, the request being for the unauthenticated code.

27. (Original) The computer program product of claim 21, further comprising:

sixth instructions for receiving the unauthenticated code again, if the first hash value and the second hash value do not match;

seventh instructions for generating a third hash value of the unauthenticated code; and

eighth instructions for comparing the first hash value and the third hash value.

28. (Original) The computer program product of claim 27, further comprising:

ninth instructions for comparing the second hash value and the third hash value, if the third hash value and the first hash value do not match; and

tenth instructions for determining that the unauthenticated code has been corrupted intentionally, if the second hash value and the third hash value match.

29. (Original) The computer program product of claim 28, further comprising eleventh instructions for determining that the unauthenticated code has been corrupted unintentionally, if the second hash value and the third hash value do not match.